

10/518499

Rec'd PCT/PTO 2003 DEC 7 2004

11.07.03

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 6月19日

出 願 番 号

Application Number:

特願2002-178947

[ST.10/C]:

[JP2002-178947]

出 願 人

Applicant(s):

株式会社エイシーエス

REC'D 01 AUG 2003

WIPO PAT

**PRIORITY
DOCUMENT**

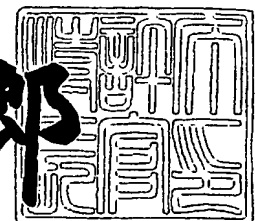
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

2003年 6月13日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3046358

【書類名】 特許願

【整理番号】 COP-00833

【提出日】 平成14年 6月19日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 1/00

【発明者】

【住所又は居所】 神奈川県川崎市中原区新丸子 9 1 5 - 1 5 株式会社エ
イシーエス内

【氏名】 大河 克好

【発明者】

【住所又は居所】 神奈川県川崎市中原区新丸子 9 1 5 - 1 5 株式会社エ
イシーエス内

【氏名】 橋本 努

【特許出願人】

【識別番号】 500196087

【氏名又は名称】 株式会社エイシーエス

【代理人】

【識別番号】 100079049

【弁理士】

【氏名又は名称】 中島 淳

【電話番号】 03-3357-5171

【代理人】

【識別番号】 100084995

【弁理士】

【氏名又は名称】 加藤 和詳

【電話番号】 03-3357-5171

【代理人】

【識別番号】 100085279

【弁理士】

【氏名又は名称】 西元 勝一

【電話番号】 03-3357-5171

【代理人】

【識別番号】 100099025

【弁理士】

【氏名又は名称】 福田 浩志

【電話番号】 03-3357-5171

【手数料の表示】

【予納台帳番号】 006839

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 相互認証方法

【特許請求の範囲】

【請求項1】 通信回線を介して接続された第1認証装置と第2認証装置の相互関係を認証する相互認証方法であって、

前記第1認証装置を特定するための記憶データと、第2認証装置を特定するための記憶データとを、前記第1認証装置及び第2認証装置の間で予め相互になされた認証による認証毎に前回の認証による記憶データを用いて更新した更新結果を履歴データとして、前記第1認証装置及び第2認証装置の各々に共通に記憶する記憶工程と、

前記第1認証装置は、記憶されている履歴データを用いて記憶データを新規に生成しかつ生成した新規の記憶データを前記履歴データを用いて暗号化して第2認証装置に送信する第1送信工程と、前記第2認証装置からの記憶データ及び前記送信した新規の記憶データによって前記履歴データを更新する第1更新工程と、を含み、

前記第2認証装置は、前記第1認証装置からの記憶データ及び記憶されている履歴データを用いて新規に記憶データを生成しかつ生成した新規の記憶データを前記履歴データを用いて暗号化して第1認証装置に送信する第2送信工程と、前記第1認証装置からの記憶データ及び前記送信した新規の記憶データによって前記履歴データを更新する第2更新工程とを含み、

前記第1認証装置及び第2認証装置の少なくとも一方の装置において、履歴データに基づいて記憶データの正当性が成立したときに、第1認証装置と第2認証装置の相互関係が正当であると検証する

ことを特徴とする相互認証方法。

【請求項2】 前記履歴データを履歴データKとして、該履歴データKとして記憶する、前記第1認証装置を特定するための記憶データは、暗証データC及び認証データRであり、前記第2認証装置を特定するための記憶データは、暗証データS及び認証データQであることを特徴とする請求項1に記載の相互認証方

法。

【請求項3】 前記第1送信工程は、記憶されている履歴データKの暗証データS及び認証データRを用いて暗証データCを新規に生成しかつ、記憶されている履歴データKの認証データRについて新規に生成し、生成した新規の認証データRを前記履歴データKを用いて暗号化して認証データAを求め、前記認証データA及び新規の暗証データCを第2認証装置に送信し、

前記第1更新工程は、前記第2認証装置からのデータを受信し、前記送信した新規の暗証データC、受信した新規に生成された暗証データS、受信した新規に生成された認証データQ、及び前記送信した新規の認証データRにより、前記履歴データKを更新し、

前記第2送信工程は、前記第1認証装置からのデータを受信し、受信した新規の暗証データC及び記憶されている履歴データKの認証データQを用いて暗証データSを新規に生成しかつ記憶されている履歴データKの認証データQについて新規に生成し、生成した新規の認証データQを記憶した履歴データKを用いて暗号化して認証データBを求め、前記認証データB及び新規の暗証データSを第1認証装置に送信し、

前記第2更新工程は、受信した新規の暗証データC、新規に生成した暗証データS、新規に生成した認証データQ、及び受信した新規の認証データRにより、前記履歴データKを更新し、

前記第1認証装置及び第2認証装置の少なくとも一方の装置において、履歴データKに基づいて暗証データの正当性が成立したときに、第1認証装置と第2認証装置の相互関係が正当であると検証する

ことを特徴とする請求項2に記載の相互認証方法。

【請求項4】 前記記憶工程は、前記第1送信工程、第1更新工程、第2送信工程、及び第2更新工程における認証による更新結果を履歴データとして記憶することを特徴とする請求項1乃至請求項3の何れか1項に記載の相互認証方法

【請求項5】 前記認証データR及び認証データQの少なくとも一方は、乱数発生手段により発生された乱数、データ容量、時間データの少なくとも1つで

あることを特徴とすることを特徴とする請求項 2 に記載の相互認証方法。

【請求項 6】 前記第 1 認証装置の第 1 送信工程では、前記暗証データ S 及び認証データ R による予め定めた関数の演算結果の値を暗証データ C として生成し、前記第 2 認証装置の第 2 送信工程では、前記暗証データ C 及び前記認証データ Q による予め定めた関数の演算結果の値を暗証データ S として生成することを特徴とする請求項 2 に記載の相互認証方法。

【請求項 7】 前記第 1 認証装置の第 1 送信工程では、前記生成した新規の認証データ R 及び前記履歴データ K による予め定めた関数の演算結果の値を認証データ A として求め、前記第 2 認証装置の第 2 送信工程では、前記生成した新規の認証データ Q 及び前記履歴データ K による予め定めた関数の演算結果の値を認証データ B として求めることを特徴とする請求項 2 に記載の相互認証方法。

【請求項 8】 前記第 1 認証装置の検証工程は、前記履歴データ K のうち記憶されている認証データ Q 及び前回送信する前に生成した暗証データ C による予め定めた関数の演算結果の値が受信した暗証データ S と一致するときに前記相互関係が正当であると検証することを特徴とする請求項 2 に記載の相互認証方法。

【請求項 9】 前記第 2 認証装置の検証工程は、前記履歴データ K のうち記憶されている暗証データ S 及び認証データ R による予め定めた関数の演算結果の値が受信した暗証データ C と一致するときに前記相互関係が正当であると検証することを特徴とする請求項 2 に記載の相互認証方法。

【請求項 10】 前記記憶工程は、前記第 1 送信工程、第 2 送信工程、第 1 更新工程及び第 2 更新工程を複数実施した結果、得られるデータを履歴データ K として記憶することを特徴とする請求項 2 に記載の相互認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークに接続されたコンピュータシステム等の装置における相互認証方法にかかり、特に、少なくとも第 1 認証装置と第 2 認証装置との間の関係についての正当性を検証する相互認証方法に関する。

【0002】

【従来の技術】

ネットワーク上において、あるユーザが自分の身元を証明するためには、認証が必要である。認証とは、何らかのプロトコルにより、証明者が自分の身元を検証者に対して証明することであり、電子商取引などの分野において、必須の技術である。例えば、ユーザがサーバに対して、身元を証明したいときは、ユーザが証明者に、サーバが検証者に対応する。また、逆に、サーバがユーザに対して身元を証明したい場合は、サーバが証明者に、ユーザが検証者に対応する。1対1の装置の間では、その立場が反転する場合があるので、相互に認証する相互認証が必要である。

【0003】

相互認証は、ユーザとサーバの間に限定されず、任意のコンピュータ間での身元を証明する方法として、幅広く利用されている。最近では、公開鍵暗号を用いたものが知られており、証明者は公開鍵と秘密鍵を所持しており、証明者が公開鍵に対応する秘密鍵を所持することを、なんらかのプロトコルにより、検証者に示すことにより、身元を証明している。

【0004】

【発明が解決しようとする課題】

しかしながら、従来の相互認証方法では、認証に用いる鍵が単一であるため、ひとたび鍵が知られてしまうと、第三者がユーザになりすまして認証される場合がある。また、ユーザは、鍵の保管に注意を払わなければならない、簡便に利用することができなかった。

【0005】

例えば、インターネットのような非同期型ネットワークでは、複数のコンピュータが同時に通信しており、証明者が複数の検証者と同時にプロトコルを実行する場合がある。WWW (World Wide Web: ワールド・ワイド・ウェブ) では、HTTP (Hypertext Transfer Protocol : WWWサーバとWWWブラウザやWebブラウザ等が、ファイル等の情報授受に使うプロトコル) のサーバと、接続先であるクライアントとの間では、多数の認証が要求される。

【0006】

本発明は、上記事実を考慮して、安全かつ簡便に相互認証することができる相互認証方法を得ることが目的である。

【0007】

【課題を解決するための手段】

上記目的を達成するために本発明は、通信回線を介して接続された第1認証装置と第2認証装置の相互関係を認証する相互認証方法であって、前記第1認証装置を特定するための記憶データと、第2認証装置を特定するための記憶データとを、前記第1認証装置及び第2認証装置の間で予め相互になされた認証による認証毎に前回の認証による記憶データを用いて更新した更新結果を履歴データとして、前記第1認証装置及び第2認証装置の各々に共通に記憶する記憶工程と、前記第1認証装置は、記憶されている履歴データを用いて記憶データを新規に生成しかつ生成した新規の記憶データを前記履歴データを用いて暗号化して第2認証装置に送信する第1送信工程と、前記第2認証装置からの記憶データ及び前記送信した新規の記憶データによって前記履歴データを更新する第1更新工程と、を含み、前記第2認証装置は、前記第1認証装置からの記憶データ及び記憶されている履歴データを用いて新規に記憶データを生成しかつ生成した新規の記憶データを前記履歴データを用いて暗号化して第1認証装置に送信する第2送信工程と、前記第1認証装置からの記憶データ及び前記送信した新規の記憶データによって前記履歴データを更新する第2更新工程とを含み、前記第1認証装置及び第2認証装置の少なくとも一方の装置において、履歴データに基づいて記憶データの正当性が成立したときに、第1認証装置と第2認証装置の相互関係が正当であると検証する。

【0008】

本発明では、第1認証装置を特定するための記憶データと、第2認証装置を特定するための記憶データとを、履歴データとして、前記第1認証装置及び第2認証装置の各々に共通に記憶する。この履歴データは、第1認証装置及び第2認証装置の間で予め相互になされた認証による認証毎に前回の認証による記憶データを用いて更新した更新結果である。第1認証装置は、記憶されている履歴データを用いて新規の記憶データを生成しかつ新規の記憶データを記憶されている履歴

データを用いて暗号化して第2認証装置に送信する。これを第2認証装置が受け取り、第2認証装置は第1認証装置からの記憶データ及び記憶されている履歴データを用いて新規の記憶データを生成しかつ新規の記憶データを記憶されている履歴データを用いて暗号化して第1認証装置に送信する。このとき、第1認証装置は、第2認証装置からの記憶データ及び送信した新規の記憶データによって履歴データを更新する。また、第2認証装置は、第1認証装置からの記憶データ及び送信した新規の記憶データによって履歴データを更新する。この送信工程の後には、第1認証装置及び第2認証装置の少なくとも一方の装置において、履歴データに基づいて記憶データの正当性が成立したときに、第1認証装置と第2認証装置の相互関係が正当であると検証する。すなわち、第1認証装置及び第2認証装置の一方の認証装置では、他方の認証装置からの履歴を含むデータを受け取り、記憶されている履歴データと照合することが可能となる。そして送信するときには、記憶されている履歴データから新規で異なる履歴データに基づくデータを送信するので、同一データによる授受はない。このため、秘匿性を向上させることもできる。

【 0 0 0 9 】

より詳細には、前記履歴データを履歴データKとして、該履歴データKとして記憶する、前記第1認証装置を特定するための記憶データは、暗証データC及び認証データRであり、前記第2認証装置を特定するための記憶データは、暗証データS及び認証データQであることを特徴とする。

【 0 0 1 0 】

前記第1送信工程は、記憶されている履歴データKの暗証データS及び認証データRを用いて暗証データCを新規に生成しかつ、記憶されている履歴データKの認証データRについて新規に生成し、生成した新規の認証データRを前記履歴データKを用いて暗号化して認証データAを求め、前記認証データA及び新規の暗証データCを第2認証装置に送信し、前記第1更新工程は、前記第2認証装置からのデータを受信し、前記送信した新規の暗証データC、受信した新規に生成された暗証データS、受信した新規に生成された認証データQ、及び前記送信した新規の認証データRにより、前記履歴データKを更新し、前記第2送信工程は

、前記第1認証装置からのデータを受信し、受信した新規の暗証データC及び記憶されている履歴データKの認証データQを用いて暗証データSを新規に生成し、かつ記憶されている履歴データKの認証データQについて新規に生成し、生成した新規の認証データQを記憶した履歴データKを用いて暗号化して認証データBを求め、前記認証データB及び新規の暗証データSを第1認証装置に送信し、前記第2更新工程は、受信した新規の暗証データC、新規に生成した暗証データS、新規に生成した認証データQ、及び受信した新規の認証データRにより、前記履歴データKを更新し、前記第1認証装置及び第2認証装置の少なくとも一方の装置において、履歴データKに基づいて暗証データの正当性が成立したときに、第1認証装置と第2認証装置の相互関係が正当であると検証することを特徴とする。

【0011】

前記記憶工程は、前記第1送信工程、第1更新工程、第2送信工程、及び第2更新工程における認証による更新結果を履歴データとして記憶することを特徴とする。

【0012】

前記認証データR及び認証データQの少なくとも一方は、乱数発生手段により発生された乱数、データ容量、時間データの少なくとも1つであることを特徴とする。

【0013】

前記第1認証装置の第1送信工程では、前記暗証データS及び認証データRによる予め定めた関数の演算結果の値を暗証データCとして生成し、前記第2認証装置の第2送信工程では、前記暗証データC及び前記認証データQによる予め定めた関数の演算結果の値を暗証データSとして生成することを特徴とする。

【0014】

前記第1認証装置の第1送信工程では、前記生成した新規の認証データR及び前記履歴データKによる予め定めた関数の演算結果の値を認証データAとして求め、前記第2認証装置の第2送信工程では、前記生成した新規の認証データQ及び前記履歴データKによる予め定めた関数の演算結果の値を認証データBとして

求めることを特徴とする。

【0015】

前記第1認証装置の検証工程は、前記履歴データKのうち記憶されている認証データQ及び前回送信する前に生成した暗証データCによる予め定めた関数の演算結果の値が受信した暗証データSと一致するときに前記相互関係が正当であると検証することを特徴とする。

【0016】

前記第2認証装置の検証工程は、前記履歴データKのうち記憶されている暗証データS及び認証データRによる予め定めた関数の演算結果の値が受信した暗証データCと一致するときに前記相互関係が正当であると検証することを特徴とする。

【0017】

前記記憶工程は、前記第1送信工程、第2送信工程、第1更新工程及び第2更新工程を複数実施した結果、得られるデータを履歴データKとして記憶することを特徴とする。

【0018】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態の一例を詳細に説明する。本実施の形態は、ネットワークにおいてサーバ・コンピュータとクライアント・コンピュータとの間で相互認証する場合に本発明を適用したものである。

【0019】

図2には、本発明が適用可能なネットワーク・システムの概略構成が示されている。ネットワークシステムは、CPUを少なくとも含む一または複数のクライアント・コンピュータ10、及びCPUを少なくとも含む一または複数のサーバ・コンピュータ40が、それぞれモデム、ルータ、TA（ターミナル・アダプタ：Terminal Adapter）等を介して、ネットワーク（例えば、インターネット）32に接続されて構成されている。これらのコンピュータは、ネットワーク32を介して、相互通信により情報授受が可能である。

【0020】

なお、図2に示すように、クライアント・コンピュータ10及びサーバ・コンピュータ40の各々は1つのコンピュータとして説明するが、これらのクライアント・コンピュータ10、サーバ・コンピュータ40は複数台でもよい。

【0021】

なお、クライアント・コンピュータ10が本発明の第1認証装置に相当するとき、サーバ・コンピュータ40が第2認証装置に相当し、サーバ・コンピュータ40が本発明の第1認証装置に相当するとき、クライアント・コンピュータ10が第2認証装置に相当する。また、ネットワーク32は本発明の通信回線に相当する。

【0022】

本実施の形態では、ネットワークとしてインターネットを適用した場合を説明する。この場合、少なくとも1つのコンピュータは、WWW (World Wide Web) サーバとして機能させることができ、また他のマシンはWWWクライアントとして機能させることもできる。

【0023】

詳細には、各クライアント・コンピュータ10には、WWWブラウザがインストールされており、このWWWブラウザを起動することにより、ネットワーク32を介してサーバ・コンピュータ40に任意にアクセス可能となる。このとき、アクセス位置（アクセス先のサーバ・コンピュータ40の位置、及びサーバ・コンピュータ40内の情報の位置で構成されるデータ）は、URL (Uniform Resource Locator) で指定される。

【0024】

サーバ・コンピュータ40は、クライアント・コンピュータ10からアクセス要求があった場合、URLで指定された位置にあるデータを、ネットワーク32を介して、アクセス元のクライアント・コンピュータ10へ送信する。このとき、データは、一般に、HTTP (Hyper Text Transfer Protocol) に従って転送される。

【0025】

なお、クライアント・コンピュータ10の識別には、IP (Internet Protoco

1) アドレスが用いられる。また、クライアント・コンピュータ10を操作するユーザの識別には、ユーザ自身の入力や、予め定められているコード等のユーザIDを用いることができる。

【0026】

上記コンピュータには、当該コンピュータで指示入力をするために、各々キーボード、マウス等の入力装置が設けられており、コンピュータによる処理結果等を表示するためにディスプレイが設けられている。なお、コンピュータは、汎用的かつ一般的なハードウェア構成であるため、詳細な説明を省略する。

【0027】

クライアント・コンピュータ10は、システムパラメータ等を入力するための入力装置12を備えており、入力装置12は入力に応じた乱数Rを発生する乱数発生器14及びメモリ16に接続されている。乱数発生器14は、メモリ16及び乱数Rに基づく認証用データAを求める認証用データ演算器18に接続されている。認証用データ演算器18は、ネットワーク32を介してサーバ・コンピュータ40と通信するためにネットワーク32に接続された通信インタフェース（以下、通信I/Fという）30に接続されている。

【0028】

通信I/F30には、検証器20が接続されている。この検証器20はメモリ16及び認証用データ演算器18にも接続されている。また、検証器20は、サーバ・コンピュータ40との間で認証したときに、認証により相互関係が正当であると判定されたことを表示するOK装置22及び認証により相互関係が不当であると判定されたことを表示するNG装置24にも接続されている。

【0029】

サーバ・コンピュータ40は、システムパラメータ等を入力するための入力装置42を備えており、入力装置42は入力に応じた乱数Qを発生する乱数発生器44及びメモリ46に接続されている。乱数発生器44は、メモリ46及び乱数Rに基づく認証用データBを求める認証用データ演算器48に接続されている。認証用データ演算器48は、ネットワーク32を介してクライアント・コンピュータ10と通信するために通信I/F60に接続されている。

【 0 0 3 0 】

通信 I / F 6 0 には、検証器 5 0 が接続されている。この検証器 5 0 はメモリ 4 6 及び認証用データ演算器 4 8 にも接続されている。また、検証器 5 0 は、クライアント・コンピュータ 1 0 との間で認証したときに、認証により相互関係が正当であると判定されたことを表示する OK 装置 5 2 及び認証により相互関係が不当であると判定されたことを表示する NG 装置 5 4 にも接続されている。

【 0 0 3 1 】

〔概念プロセス〕

次に、本実施の形態のネットワーク・システムにおける相互認証の概念プロセスを説明する。本実施の形態では、コンピュータ間の相互認証をデジタルデータの授受で実行する。図 3 には、相互認証の概念プロセスをフローチャートとして示した。

【 0 0 3 2 】

ステップ 1 0 0 では、クライアント・コンピュータ 1 0 及びサーバ・コンピュータ 4 0 は、予め定めた手順により、双方に共通な初期値（隠蔽鍵 K_0 ）を記憶する。

【 0 0 3 3 】

予め定めた手順とは、クライアント・コンピュータ 1 0 及びサーバ・コンピュータ 4 0 の間の相互認証を実行するときの初期値を設定するものである。例えば、クライアント・コンピュータ 1 0 及びサーバ・コンピュータ 4 0 に共通なデータを初期値として保持させるため、クライアント・コンピュータ 1 0 及びサーバ・コンピュータ 4 0 の何れか一方、または第三者のコンピュータによって定められる初期値を、クライアント・コンピュータ 1 0 及びサーバ・コンピュータ 4 0 の双方へ提供する。この提供は、初期値を電子メールなどの電子的にデータ送信することや、初期値を印刷した印刷物をクライアント・コンピュータ 1 0 及びサーバ・コンピュータ 4 0 の双方に送付してクライアント・コンピュータ 1 0 及びサーバ・コンピュータ 4 0 の各々で入力することによって達成される。

【 0 0 3 4 】

本実施の形態では、この初期値として、クライアント・コンピュータ 1 0 及び

サーバ・コンピュータ40の双方で共通な状態を維持するため、クライアント・コンピュータ10とサーバ・コンピュータ40との間でなされるデータ授受の履歴を初期値とし、後のクライアント・コンピュータ10とサーバ・コンピュータ40との間でなされるデータ授受毎に初期値を更新する。

【0035】

すなわち、上記初期値は、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方に共通な値であればよく、上記のように任意の値を提供することで双方で保持してもよいが、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方で共通な状態を維持するため、任意のアルゴリズムによるクライアント・コンピュータ10及びサーバ・コンピュータ40の間のデータ授受の結果が好ましい。本実施の形態では、任意のアルゴリズムには、送信側と受信側との双方のデータを送信側及び受信側の双方で共通に保持する手順で可能であり、詳細を後述する相互認証の結果のデータを用いている。

【0036】

なお、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方に記憶するデータの形式（例えばフォーマット）は、同一に限定するものではない。すなわち、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方に記憶するデータは、そのデータの最終的な値が同一であればよく、データそのものの同一性に限定されない。例えば、異なる形式で格納するようにしてもよい。このようにすれば、一方のデータが漏洩した場合であっても、他方のデータは維持可能となる。

【0037】

まず、ステップ110では、クライアント・コンピュータ10が、認証データを送付する。この認証データは、クライアント・コンピュータ10からサーバ・コンピュータ40に対して相互認証を要求する最初のデータであり、記憶されている初期値を隠蔽鍵として用い、クライアント・コンピュータ10内で生成されるデータを記憶すると共に隠蔽鍵による暗号化を行って、送付する。

【0038】

次に、ステップ120では、サーバ・コンピュータ40において、クライアン

ト・コンピュータ10から送付された認証データを受け取って、記憶されている初期値を隠蔽鍵として用い、この時点でサーバ・コンピュータ40内で生成されるデータを記憶すると共に隠蔽鍵による暗号化を行った認証データを送付する。なお、認証データには、クライアント・コンピュータ10から受け取った認証データに含まれる一部のデータを含ませる。

【0039】

これにより、サーバ・コンピュータ40から送付する認証データがクライアント・コンピュータ10からの要求に対する応答であることを表すデータとして送付することができる。この認証データを送付した後は、受け取った認証データを解析すると共に、サーバ・コンピュータ40内で生成したデータの各々を用いて新規の隠蔽鍵を生成すると共に、新規の隠蔽鍵で、記憶されている隠蔽鍵を更新する。

【0040】

次に、ステップ130では、クライアント・コンピュータ10において、サーバ・コンピュータ40から送付された認証データを受け取って、記憶されている初期値を隠蔽鍵として用い、この時点でクライアント・コンピュータ10内で生成されるデータを記憶すると共に隠蔽鍵による暗号化を行った認証データを送付する。なお、認証データには、サーバ・コンピュータ40から受け取った認証データに含まれる一部のデータを含ませる。

【0041】

これにより、クライアント・コンピュータ10から送付する認証データがサーバ・コンピュータ40から送付されたものに対する応答であることを表すデータとして送付することができる。この認証データを送付した後は、受け取った認証データを解析すると共に、クライアント・コンピュータ10内で生成したデータの各々を用いて新規の隠蔽鍵を生成すると共に、新規の隠蔽鍵で、記憶されている隠蔽鍵を更新する。

【0042】

従って、ステップ130のプロセスが終了した時点で、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方において、初期値（隠蔽鍵）が

更新されて、共通の値（隠蔽鍵）として維持することができる。

【0043】

次のステップ140では、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方のプロセスが予め定めた所定回数を完了したか否かを判断する。この判断基準回数は、少なくとも1回の回数が予め設定されており、本実施の形態では、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方に共通の回数の値が保持される。なお、判断基準回数は、クライアント・コンピュータ10及びサーバ・コンピュータ40の各々で異なる回数の値を保持してもよい。この場合には、クライアント・コンピュータ10及びサーバ・コンピュータ40の各々で認証の基準が異なることになるが、認証が正当であれば判断基準回数が少ないコンピュータ側で複数回のデータ授受が要求されることのみで達成できる。この回数を参照することで、クライアント・コンピュータ10では、ステップ140の更新処理、サーバ・コンピュータ40ではステップ120の更新処理が保持されている回数を終了するまで否定される。判断基準回数が1回に設定されている場合には、ステップ140で否定されることなく、そのままステップ150へ進む。

【0044】

従って、ステップ140で肯定判断された時点で、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方において、共に値（隠蔽鍵）が更新されて、双方で共通の値（隠蔽鍵）が維持されることになる。すなわち、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方で保持する隠蔽鍵が情報授受毎に新規なものに更新され、常時最新の隠蔽鍵として維持することができる。

【0045】

ステップ150では、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方において、認証処理が実行されて本プロセスを終了する。

【0046】

上記認証処理は、記憶されている最新の隠蔽鍵を用いて、送付された認証データが正当かデータであるか否かを判別することによってなされる。この認証処理

は、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方において共通に実行できる。この認証処理が完了すると、クライアント・コンピュータ10及びサーバ・コンピュータ40の双方において相互認証が完了したことになる。

【0047】

〔詳細プロセス〕

次に、上記概念プロセスで述べた相互認証を詳細に説明する。

【0048】

(隠蔽鍵を含むデータの構成)

本実施の形態では、隠蔽鍵は、情報授受毎に最新データに更新されるため、履歴データKとして機能する。以下の説明では、この履歴データKとして機能するものとして隠蔽鍵Kを同一表記とする。

【0049】

上記概念プロセスで認証データとして用いる初期値を含む隠蔽鍵Kは、クライアント・コンピュータ10を特定するための暗証データC及び認証データRと、サーバ・コンピュータ40を特定するための暗証データS及び認証データQと、から構成される。なお、以下の説明では、隠蔽鍵K、暗証データC、認証データR、暗証データS及び認証データQに初期値「0」から増加する添え字を付し、更新状態を表すものとするが、これらを一般的に説明する場合には添え字を削除した記号のみを用いて説明する。

【0050】

本実施の形態では、初期値として、詳細を後述するクライアント・コンピュータ10及びサーバ・コンピュータ40の双方でなされたデータ授受の結果を記憶するものとし、既に履歴データが内在するものとする。

【0051】

隠蔽鍵Kは、暗証データC、認証データR、暗証データS及び認証データQの各々を用いた関数 $g(C, S, Q, R)$ の計算結果を用いる。関数 g は、単純和や係数付加の多項式、乗算、積和そしてハッシュ関数が一例としてある。

【0052】

また、クライアント・コンピュータ10側の初期値 C_0 , R_0 を生成するための最初の値は、暗証データC及び認証データRについてユーザが設定した値を用いてもよく、自動的に生成してもよい。認証データRは情報授受毎に内容が無規則で変動することが好ましいので、本実施の形態では、認証データRとして乱数発生器14で発生された乱数を用いている。しかし、本発明は、認証データRに乱数を用いることに限定されるものではない。例えば、現在年月日、日時、時刻などの時間データ、コンピュータ内に格納された任意ファイル容量やタイムスタンプ、及び情報授受のときの容量などを用いることができる。

【0053】

同様に、サーバ・コンピュータ40側の初期値 S_0 , Q_0 を生成するための最初の値は、暗証データS及び認証データQについてサーバ・コンピュータ40を管理するオペレータが設定した値を用いてもよく、自動的に生成してもよい。上記と同様に認証データQは情報授受毎に内容が無規則で変動することが好ましいので、本実施の形態では、認証データQとして乱数発生器44で発生された乱数を用いている。しかし、本発明は、認証データQに乱数を用いることに限定されるものではない。例えば、現在年月日、日時、時刻などの時間データ、コンピュータ内に格納された任意ファイル容量やタイムスタンプ、及び情報授受のときの容量などを用いることができる。

【0054】

また、クライアント・コンピュータ10側の認証データR、及びサーバ・コンピュータ40側の認証データQを他方へ送信するが、その送信データについて第三者による特定を困難にするため、秘匿する必要がある。そこで、本実施の形態では、クライアント・コンピュータ10からサーバ・コンピュータ40へ送信する認証データR、及びサーバ・コンピュータ40からクライアント・コンピュータ10へ送信する認証データQを隠蔽鍵Kで隠蔽する。

【0055】

すなわち、クライアント・コンピュータ10からサーバ・コンピュータ40へ送信する場合、予め定めた関数 $v(R, K)$ により認証データAを生成して送信する。関数 v は、単純和や係数付加の多項式、乗算、積和そしてハッシュ関数が

一例としてある。同様に、サーバ・コンピュータ40からクライアント・コンピュータ10へ送信する場合も、予め定めた関数 $w(Q, K)$ により認証データ B を生成して送信する。関数 w は、単純和や係数付加の多項式、乗算、積和そしてハッシュ関数が一例としてある。次に、関数 v 、 w の一例を示す。

【0056】

$$A_m = v(R, K) = R_m + K_{m-1}$$

$$B_m = w(Q, K) = Q_m + K_{m-1}$$

ただし、 $m \geq 1$ の自然数である。

【0057】

また、クライアント・コンピュータ10側の暗証データ C 、及びサーバ・コンピュータ40側の暗証データ S を他方へ送信するが、以下に説明するように、暗証データは情報授受の度に変更している。すなわち、クライアント・コンピュータ10からサーバ・コンピュータ40へ送信する暗証データ C は、その送信するときに予め定めた関数 $y(S, R)$ により新規の暗証データ C を生成して送信する。関数 y は、単純和や係数付加の多項式、乗算、積和そしてハッシュ関数が一例としてある。同様に、サーバ・コンピュータ40からクライアント・コンピュータ10へ送信する場合も、予め定めた関数 $z(C, Q)$ により暗証データ S を生成して送信する。関数 z は、単純和や係数付加の多項式、乗算、積和そしてハッシュ関数が一例としてある。次に、関数 y 、 z の一例を示す。

【0058】

$$C_m = y(S, R) = S_{m-1} + R_{m-1}$$

$$B_m = w(C, Q) = C_{m-1} + Q_{m-1}$$

ただし、 $m \geq 1$ の自然数である。

【0059】

なお、暗証データの送信では、第三者による特定を困難にするため、秘匿してもよい。例えば、クライアント・コンピュータ10からサーバ・コンピュータ40へ送信する暗証データ C 、及びサーバ・コンピュータ40からクライアント・コンピュータ10へ送信する暗証データ S を隠蔽鍵 K で隠蔽するようにしてもよい。すなわち、隠蔽鍵 K をパラメータとして追加した関数にしてもよい。

【0060】

(詳細プロセス)

次に、図1を参照して本実施の形態の詳細プロセスを説明する。

ステップP0：クライアント・コンピュータ10及びサーバ・コンピュータ40の各々に、初期値の隠蔽鍵 K_0 を格納する。このプロセスは、図3のステップ100と、図1のプロセスPc0及びPs0に相当する。

【0061】

ステップP1：クライアント・コンピュータ10では、乱数Rを生成し、暗証データC及び認証データAを計算し、サーバ・コンピュータ40に送信する。このプロセスは、図3のステップ110と、図1のプロセスPc1に相当する。

【0062】

すなわち、クライアント・コンピュータ10では、乱数発生器14において乱数 R_1 を生成する。生成された乱数 R_1 、メモリ16に記憶されている隠蔽鍵 K_0 及び隠蔽鍵 K_0 を構成する C_0 、 S_0 、 Q_0 、 R_0 は認証用データ演算器18へ入力される。そして、認証用データ演算器18は、その乱数 R_1 及びメモリ16に記憶されている隠蔽鍵 K_0 及び隠蔽鍵 K_0 を構成する暗証データ S_0 、認証データ R_0 を用いて上記関数 y 、 v により新規の暗証データ C_1 、及び新規の認証データ A_1 を求める。この求めた新規の暗証データ C_1 、及び認証データ A_1 はメモリ16に記憶すると共に、通信I/F30に出力され、ネットワーク32を介してサーバ・コンピュータ40へ送信される。この送信データは、図1のデータDc1に相当する。

【0063】

ステップP2：サーバ・コンピュータ40は、クライアント・コンピュータ10から認証データA及び暗証データCを受信すると共に、乱数Qを生成し暗証データS、認証データQを計算しクライアント・コンピュータ10に送信する。これと共に、記憶されている隠蔽鍵 K_0 を新規の隠蔽鍵 K_1 に更新する。このプロセスは、図3のステップ120と、図1のプロセスPs1に相当する。

【0064】

すなわち、サーバ・コンピュータ40では、通信I/F60を介して検証器5

0にクライアント・コンピュータ10からの暗証データ C_1 及び認証データ A_1 が入力される。このとき、サーバ・コンピュータ40では、乱数発生器44において乱数 Q_1 を生成する。生成された乱数 Q_1 、メモリ46に記憶されている隠蔽鍵 K_0 及び隠蔽鍵 K_0 を構成する C_0 、 S_0 、 Q_0 、 R_0 は認証用データ演算器48へ入力される。また、検証器50は、クライアント・コンピュータ10からの暗証データ C_1 及び認証データ A_1 を認証用データ演算器48へ出力する。

【0065】

認証用データ演算器48は、その乱数 Q_1 、受信した暗証データ C_1 及び記憶されている隠蔽鍵 K_0 及び隠蔽鍵 K_0 を構成する認証データ Q_0 を用いて上記関数 z 、 w により新規の暗証データ S_1 、及び新規の認証データ B_1 を求める。この求めた新規の暗証データ S_1 、及び認証データ B_1 は通信I/F60に出力され、ネットワーク32を介してクライアント・コンピュータ10へ送信される。この送信データは、図1のデータDs1に相当する。

【0066】

このとき、サーバ・コンピュータ40では、初期値としての隠蔽鍵 K_0 を構成する各データについて新規のデータが入手できている。すなわち、暗証データ C についてはクライアント・コンピュータ10から受信した暗証データ C_1 、暗証データ S については認証用データ演算器48で計算した暗証データ S_1 、認証データ Q については乱数発生器44で発生した乱数 Q_1 、認証データ R についてはクライアント・コンピュータ10から受信した認証データ A から逆算すなわち隠蔽鍵 K_0 を減算することで得られる乱数 R_1 である。

【0067】

そこで、これらの暗証データ C_1 、暗証データ S_1 、認証データ Q_1 、認証データ R_1 を、新規のデータとして更新すると共に、新規の隠蔽鍵 K_1 として更新する。これによって、サーバ・コンピュータ40では、隠蔽鍵 K の履歴として最新のデータに自動的に更新することができる。

【0068】

ステップP3：クライアント・コンピュータ10は、サーバ・コンピュータ40から認証データ B 及び暗証データ S を受信すると共に、乱数 R を生成し暗証デ

ータ C_2 、認証データ A_2 を計算しサーバ・コンピュータ 40 に送信する。これと共に、記憶されている隠蔽鍵 K_0 を新規の隠蔽鍵 K_1 に更新する。このプロセスは、図 3 のステップ 130 と、図 1 のプロセス $Pc2$ に相当する。

【0069】

すなわち、クライアント・コンピュータ 10 では、通信 I/F 30 を介して検証器 20 にサーバ・コンピュータ 40 からの暗証データ S_1 及び認証データ B_1 が入力される。このとき、クライアント・コンピュータ 10 では、乱数発生器 14 において乱数 R_2 を生成する。生成された乱数 Q_2 、メモリ 46 に記憶されている隠蔽鍵 K_0 及び隠蔽鍵 K_0 を構成する C_0 、 S_0 、 Q_0 、 R_0 は認証用データ演算器 18 へ入力される。また、検証器 20 は、サーバ・コンピュータ 40 からの暗証データ S_1 及び認証データ B_1 を認証用データ演算器 18 へ出力する。

【0070】

このとき、クライアント・コンピュータ 10 では、初期値としてメモリ 16 に記憶されている隠蔽鍵 K_0 を構成する各データについて新規のデータ（新規の隠蔽鍵 K_1 を構成するデータ）が入手できている。すなわち、暗証データ C についてはサーバ・コンピュータ 40 から受信した暗証データ S_1 から逆算すなわち隠蔽鍵 K_0 を構成したメモリ 16 に記憶されている認証データ Q_0 を減算することで得られる暗証データ C_1 、またはメモリ 16 に記憶されている前回送信した暗証データ C_1 が対応する。暗証データ S についてはサーバ・コンピュータ 40 から受信した暗証データ S_1 、認証データ Q についてはサーバ・コンピュータ 40 から受信した認証データ B_1 から逆算すなわち隠蔽鍵 K_0 を減算することで得られる認証データ Q_1 、認証データ R については前回生成した乱数 R_1 である。

【0071】

そこで、これらの暗証データ C_1 、暗証データ S_1 、認証データ Q_1 、認証データ R_1 を、新規のデータとして更新すると共に、新規の隠蔽鍵 K_1 として更新する。これによって、クライアント・コンピュータ 10 では、サーバ・コンピュータ 40 と同一の隠蔽鍵 K を、最新のデータに自動的に更新することができる。

【0072】

また、認証用データ演算器 18 は、生成した乱数 R_2 、更新した履歴データ K_1

の認証データ R_1 、受信した暗証データ S_1 及び新規の隠蔽鍵 K_1 を用いて上記関数 y 、 v により新規の暗証データ C_2 、及び新規の認証データ A_2 を求める。この求めた新規の暗証データ C_2 、及び認証データ A_2 はメモリ 16 に記憶すると共に、通信 I/F 30 に出力され、ネットワーク 32 を介してサーバ・コンピュータ 40 へ送信される。この送信データは、図 1 のデータ Dc2 に相当する。

【0073】

ステップ P4：上記ステップ P2 及び P3 のプロセスを所定回数 m だけ実行する。なお、本実施の形態では、所定回数 m は、少なくとも 1 回のデータ授受を含む。このため、繰り返しを行わない回数 ($m=1$) を含むものである。すなわち、クライアント・コンピュータ 10 とサーバ・コンピュータ 40 との間でなされるデータ授受のときには、既に双方でなされたデータ授受の履歴データが利用されるため、1 回のデータ授受であっても、その授受のときにはクライアント・コンピュータ 10 とサーバ・コンピュータ 40 との間の履歴を含んでデータ授受がなされるため、単なるデータ授受ではなく、履歴データの授受となるので有効である。上記ステップ P2 及び P3 のプロセスを複数回数だけ繰り返すことは、データの正当性の判断精度向上に有効である。

【0074】

すなわち、上記処理を繰り返すプロセスは、繰り返す回数すなわち実行回数を複数回予め定めておくことで、隠蔽鍵 K の値が更新されることで変動し、その変動を第三者が把握することを抑制することが可能になる。このように複数回とすることで、クライアント・コンピュータ 10 及びサーバ・コンピュータ 40 で共通に保持する隠蔽鍵 K は複数回数だけ今までの履歴に従って最新の状態に更新されるので、隠蔽鍵 K を導出することが困難になる。

【0075】

ステップ P2 及び P3 のプロセスを所定回数 m だけ実行した結果、クライアント・コンピュータ 10 及びサーバ・コンピュータ 40 の各々には、隠蔽鍵 K_m 及び隠蔽鍵 K_m を構成する C_m 、 S_m 、 Q_m 、 R_m の値が保持される。なお、 $m=1$ のときは、1 回のデータ授受の値が保持される。

【0076】

なお、処理を繰り返す実行プロセスは、図3のステップ140の判断によるプロセス実行と、図1のプロセスPc2からPsm及びPcmのプロセスについて、プロセスPc1からPs1及びPc2のプロセスを繰り返したことに相当する。

【0077】

ステップP5：上記プロセスが終了した後に、クライアント・コンピュータ10及びサーバ・コンピュータ40の各々では、受信したデータの正当性が成立するか否かを検査し、成立すれば相互認証が成功したものであるとして両者の関係を許諾し、非成立のときは相互認証が不成功であるとして両者の関係を拒否する。このプロセスは、図3のステップ150と、図1のプロセスPsm+1及びPcm+1に相当する。

【0078】

1回の実行の後に認証する場合には、クライアント・コンピュータ10から1回目のデータ送信がなされるが、そのときクライアント・コンピュータ10は、クライアント・コンピュータ10とサーバ・コンピュータ40との履歴を含む初期値として記憶された隠蔽鍵K0、により生成される、認証データA1、及び暗証データC1をサーバ・コンピュータ40へ送信する。このプロセスは、図1のプロセスPc1の後にデータDc1を送信することに相当する。

【0079】

サーバ・コンピュータ40では、通信I/F60を介して検証器50にクライアント・コンピュータ10からの暗証データC1及び認証データA1が入力され、暗証データC1について検証器50において正当性を検証する。受信した暗証データC1は、前回の履歴のデータに基づいて生成されているため、サーバ・コンピュータ40では、最新の状態に更新記憶されている隠蔽鍵K0（ここでは初期値）を構成する暗証データS0及び認証データR0を用いて上述の関数yの計算結果と、受信したデータが一致するか否かを判別し、一致する場合は正当性を認め不一致の場合は正当性を否定する。正当性が認められたときには、OK装置52で正当性があることを報知した後に処理を継続し、否認されたときにはNG装置54で不当であることを報知した後に処理を終了する。

【0080】

正当性が認められて処理が継続されたときには、上記ステップP2と同様にし、乱数発生器44において乱数 Q_1 を生成し、認証用データ演算器48において暗証データ S_1 、認証データ B_1 を生成して、クライアント・コンピュータ10へ送信すると共に、隠蔽鍵を最新の隠蔽鍵 K_1 に更新する。

【0081】

この認証プロセスは、図1のプロセス $P_{s_{m+1}}$ の処理に相当する。この場合、繰り返して実行していないので、 $m=0$ で処理したことに相当する。すなわち、クライアント・コンピュータ10からサーバ・コンピュータ40へデータを送信する毎に、サーバ・コンピュータ40側でクライアント・コンピュータ10から受け取った履歴を含むデータを用いて認証を行うことができる。

【0082】

一方、クライアント・コンピュータ10では、通信I/F30を介して検証器20にサーバ・コンピュータ40からの暗証データ S_1 及び認証データ B_1 が入力される。クライアント・コンピュータ10では、暗証データ S_1 について検証器20において正当性を検証する。受信した暗証データ S_1 は、暗証データCと同様に前回の履歴のデータに基づいてサーバ・コンピュータ40において生成されているため、クライアント・コンピュータ10では、最新の状態に更新記憶されている隠蔽鍵 K_0 （ここでは初期値）を構成する暗証データ C_0 及び認証データ Q_0 を用いて上述の関数 z の計算結果と、受信したデータが一致するか否かを判別し、一致する場合は正当性を認め不一致の場合は正当性を否定する。正当性が認められたときには、OK装置22で正当性があることを報知した後に処理を継続し、否認されたときにはNG装置24で不当であることを報知した後に処理を終了する。

【0083】

正当性が認められて処理が継続されたときには、クライアント・コンピュータ10とサーバ・コンピュータ40との間で実行すべき処理へと移行する。なお、クライアント・コンピュータ10では、サーバ・コンピュータ40との履歴データ K の同一性を維持するため、上記ステップP3と同様にして、隠蔽鍵を最新の

隠蔽鍵 K_1 に更新する。

【0084】

この認証プロセスは、図1のプロセス $P_{c_{m+1}}$ の処理に相当する。この場合、繰り返して実行していないので、 $m=0$ で処理したことに相当する。すなわち、サーバ・コンピュータ40からクライアント・コンピュータ10へデータを送信する毎に、クライアント・コンピュータ10側でサーバ・コンピュータ40から受け取った履歴を含むデータを用いて認証を行うことができる。

【0085】

なお、クライアント・コンピュータ10からサーバ・コンピュータ40へデータを送信する毎に、またはサーバ・コンピュータ40からクライアント・コンピュータ10へデータを送信する毎に、受け取り側で認証を行うことを含めた処理をセッションとして、この認証を含めたセッションを複数回実行してもよい。

【0086】

次に、複数回の実行を繰り返した後に認証する場合を説明する。この場合には、クライアント・コンピュータ10から m 回目のデータ送信がなされ、クライアント・コンピュータ10は、 m 回の繰り返しによって更新された隠蔽鍵 K_m により、サーバ・コンピュータ40へ認証データ A_{m+1} 、及び暗証データ C_{m+1} を送信する。このプロセスは、図1のプロセス P_{c_m} の後にデータ $D_{c_{m+1}}$ を送信することに相当する。

【0087】

まず、サーバ・コンピュータ40では、通信I/F60を介して検証器50にクライアント・コンピュータ10からの暗証データ C_{m+1} 及び認証データ A_{m+1} が入力される。サーバ・コンピュータ40では、暗証データ C_{m+1} について検証器50において正当性を検証する。受信した暗証データ C_{m+1} は、前回の履歴のデータに基づいて生成されているため、サーバ・コンピュータ40では、最新の状態に更新記憶されている隠蔽鍵 K_m を構成する暗証データ S_m 及び認証データ R_m を用いて上述の関数 y の計算結果と、受信したデータが一致するか否かを判別し、一致する場合は正当性を認め不一致の場合は正当性を否定する。正当性が認められたときには、OK装置52で正当性があることを報知した後に処理を継続し

、否認されたときにはNG装置54で不当であることを報知した後に処理を終了する。

【0088】

正当性が認められて処理が継続されたときには、上記ステップP2と同様にし、乱数発生器44において乱数 Q_{m+1} を生成し、認証用データ演算器48において暗証データ S_{m+1} 、認証データ B_{m+1} を生成して、クライアント・コンピュータ10へ送信すると共に、隠蔽鍵を最新の隠蔽鍵 K_{m+1} に更新する。この認証プロセスは、図1のプロセスP s_{m+1} の処理に相当する。

【0089】

一方、クライアント・コンピュータ10では、通信I/F30を介して検証器20にサーバ・コンピュータ40からの暗証データ S_{m+1} 及び認証データ B_{m+1} が入力される。クライアント・コンピュータ10では、暗証データ S_{m+1} について検証器20において正当性を検証する。受信した暗証データ S_{m+1} は、暗証データCと同様に前回の履歴のデータに基づいてサーバ・コンピュータ40において生成されているため、クライアント・コンピュータ10では、最新の状態に更新記憶されている隠蔽鍵 K_m を構成する暗証データ C_m 及び認証データ Q_m を用いて上述の関数 z の計算結果と、受信したデータが一致するか否かを判別し、一致する場合は正当性を認め不一致の場合は正当性を否定する。正当性が認められたときには、OK装置22で正当性があることを報知した後に処理を継続し、否認されたときにはNG装置24で不当であることを報知した後に処理を終了する。

【0090】

正当性が認められて処理が継続されたときには、クライアント・コンピュータ10とサーバ・コンピュータ40との間で実行すべき処理へと移行する。なお、クライアント・コンピュータ10では、サーバ・コンピュータ40との履歴データKの同一性を維持するため、上記ステップP3と同様にして、隠蔽鍵を最新の隠蔽鍵 K_{m+1} に更新する。この認証プロセスは、図1のプロセスP c_{m+1} の処理に相当する。

【0091】

このように、本実施の形態では、クライアント・コンピュータ10とサーバ・

コンピュータ40との間の相互認証をするときに、双方で共通の隠蔽鍵Kを有し、その隠蔽鍵Kを情報授受毎に更新している。このため、情報授受のときのデータを解析しても、認証用のデータを特定することが困難であり、秘匿性を向上することができ、確実に相互認証が可能となる。

【0092】

上記では、クライアント・コンピュータ10とサーバ・コンピュータ40との間を例にして説明したが、インターネット等の非同期ネットワークにおいては、クライアント・コンピュータ10に対してサーバ・コンピュータ40では認証が必要である。この場合には、クライアント・コンピュータ10のユーザID毎に処理を分離するようにしてもよい。

【0093】

上記プロセスは、クライアント・コンピュータ10及びサーバ・コンピュータ40の処理プログラムとして記録媒体としてのフレキシブルディスクに実行可能な形式で格納することができる。この場合、各装置に挿抜可能なフレキシブルディスクユニット(FDU)を接続して、フレキシブルディスクからFDUを介して記録された処理プログラムを実行すればよい。また、処理プログラムをコンピュータ内のRAMや他の記憶領域(例えばハードディスク装置)にアクセス可能に格納にして(インストール)して実行するようにしてもよい。また、予めROMに記憶してもよい。また、記録媒体としては、CD-ROM、MD、MO、DVD等のディスクやDAT等の磁気テープがあり、これらを用いるときには、対応する装置としてCD-ROM装置、MD装置、MO装置、DVD装置、DAT装置等を用いればよい。

【0094】

【発明の効果】

以上説明したように本発明によれば、第1認証装置及び第2認証装置の間で相互認証をするときに、第1認証装置及び第2認証装置の各々に共通に履歴データを記憶すると共に、履歴データを更新するので、安全かつ簡便に相互認証することができ、例えば、クライアント・コンピュータとサーバ・コンピュータとの間で授受される情報から、クライアント・コンピュータの鍵が漏洩することがなく、

確実に認証が行える、という効果がある。

【図面の簡単な説明】

【図 1】

本発明の実施の形態に係る相互認証における詳細プロセスを示すイメージ図である。

【図 2】

本発明の実施の形態に係るクライアント・コンピュータとサーバ・コンピュータとの概略構成を示すブロック図である。

【図 3】

本発明の実施の形態に係る相互認証における概念プロセスを示すフローチャートである。

【符号の説明】

A、B…認証データ

C、S…暗証データ

K…隠蔽鍵（履歴データ）

Q、R…認証データ

10…クライアント・コンピュータ

14…乱数発生器

16…メモリ

18…認証用データ演算器

20…検証器

22…OK装置

24…NG装置

30…通信 I/F

32…ネットワーク

40…サーバ・コンピュータ

44…乱数発生器

46…メモリ

48…認証用データ演算器

50…検証器

52…OK装置

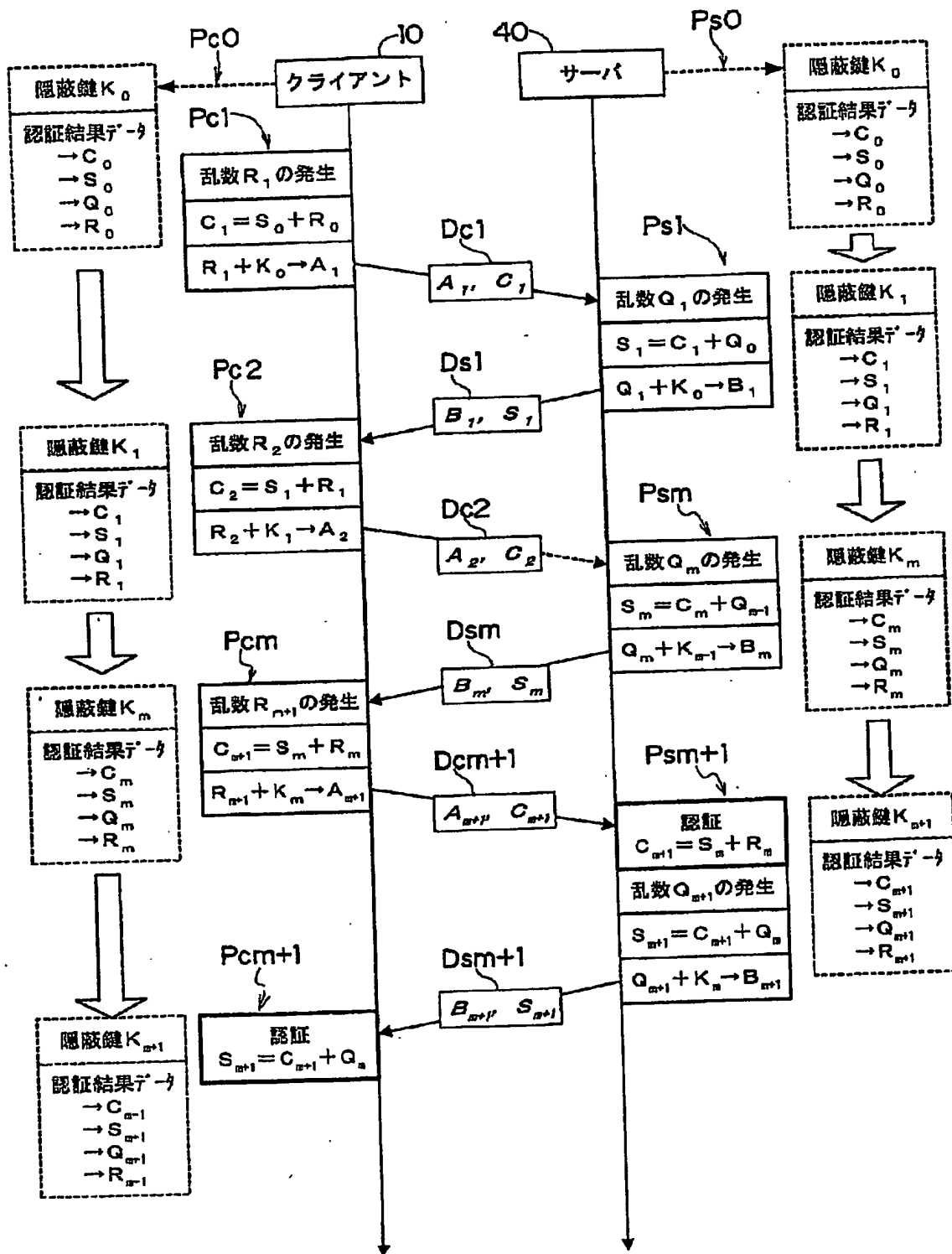
54…NG装置

60…通信I/F

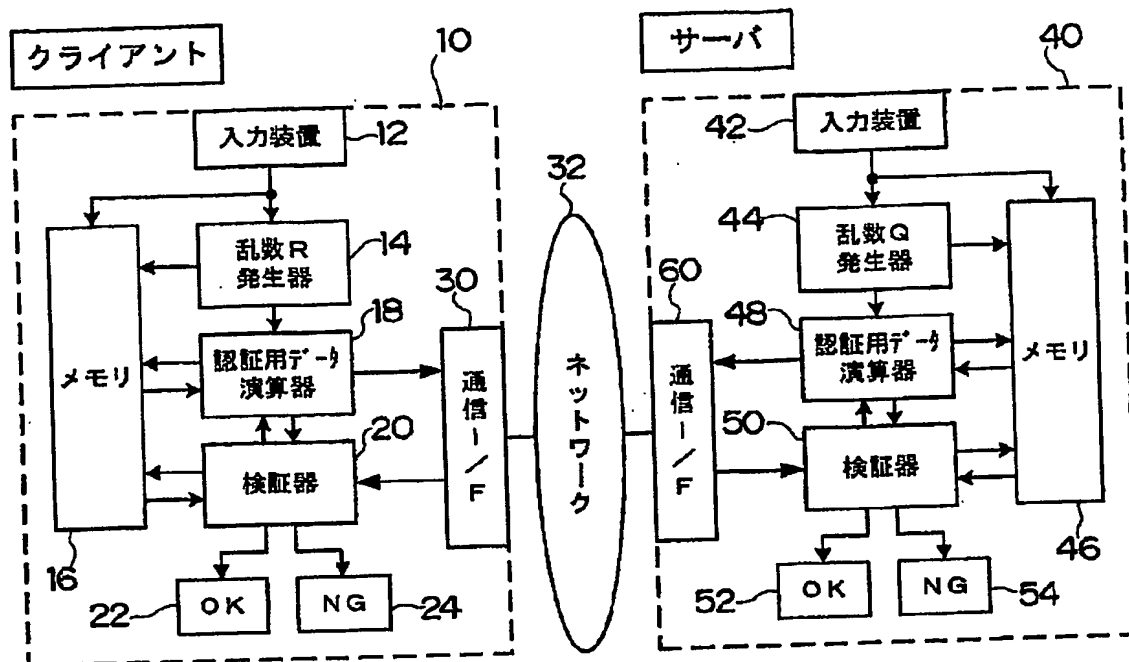
【書類名】

図面

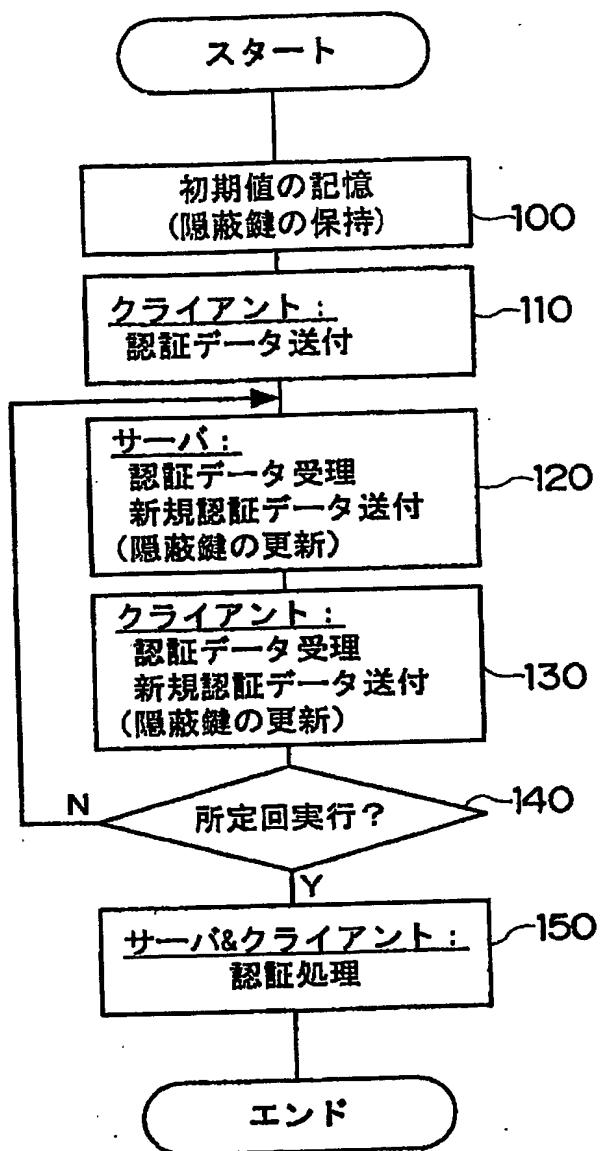
【図 1】



【図2】



【図 3】



【書類名】

要約書

【要約】

【課題】 安全かつ簡便に相互認証することができる相互認証方法を得る。

【解決手段】 相互認証プロセスにおいて、クライアント10及びサーバ40に初期値の隠蔽鍵 K_0 を格納する(Pc0、Ps0)。クライアント10は乱数Rを生成し暗証データC及び認証データAを計算し、サーバ40に送信する(Pc1)。サーバ40はクライアント10から認証データA及び暗証データCを受信しかつ乱数Qを生成し暗証データS、認証データQを計算し返信し、隠蔽鍵 K_0 を新規の隠蔽鍵 K_1 に更新する(Ps1)。クライアント10はサーバ40から認証データB及び暗証データSを受信しかつ乱数Rを生成し暗証データC₂、認証データA₂を計算しサーバ40に返信し、隠蔽鍵 K_0 を新規の隠蔽鍵 K_1 に更新する(Pc2)。クライアント10及びサーバ40は正当性が成立するか否かを検査する(Ps_{m+1}、Pc_{m+1})。

【選択図】

図1

認定・付加情報

特許出願の番号	特願2002-178947
受付番号	50200893454
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年 7月16日

<認定情報・付加情報>

【特許出願人】

【識別番号】	500196087
【住所又は居所】	神奈川県川崎市中原区新丸子915-15
【氏名又は名称】	株式会社エイシーエス

【代理人】

申請人	
【識別番号】	100079049
【住所又は居所】	東京都新宿区新宿4丁目3番17号 HK新宿ビル7階 太陽国際特許事務所
【氏名又は名称】	中島 淳

【代理人】

【識別番号】	100084995
【住所又は居所】	東京都新宿区新宿4丁目3番17号 HK新宿ビル7階 太陽国際特許事務所
【氏名又は名称】	加藤 和詳

【代理人】

【識別番号】	100085279
【住所又は居所】	東京都新宿区新宿四丁目3番17号 HK新宿ビル7階 太陽国際特許事務所
【氏名又は名称】	西元 勝一

【代理人】

【識別番号】	100099025
【住所又は居所】	東京都新宿区新宿4丁目3番17号 HK新宿ビル7階 太陽国際特許事務所
【氏名又は名称】	福田 浩志

出 願 人 履 歴 情 報

識別番号 [500196087]

1. 変更年月日 2000年 4月27日

[変更理由] 新規登録

住 所 神奈川県川崎市中原区新丸子915-15

氏 名 株式会社エイシーエス